Cisco Jabber Guestサーバ のHTML5情報漏えいの脆弱性

アドバイザリーID : Cisco-SA-20150106-CVE-2014-8024
初公開日 : 2015-01-06 21:47
バージョン 1.0 : Final
CVSSスコア : 5.0
回避策 : No Workarounds available
Cisco バグ ID : CSCus19789

CVE-2014-8024

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Jabber Guestサーバの基盤となるアプリケーションプログラミングインターフェイス(API)の脆弱性により、認証されていないリモートの攻撃者が該当システムから機密システム情報にアクセスする可能性があります。

この脆弱性は、該当ソフトウェアがHTTP GETまたはPOSTメソッドを介して渡す特定の値の検証が不十分であることに起因します。 攻撃者は、ネットワーク上のデータトラフィックをスニッフィングすることで、この脆弱性を不正利用する可能性があります。成功すると、攻撃者はシステムから機密システム情報にアクセスする可能性があります。

シスコはセキュリティ通知で脆弱性を確認していますが、ソフトウェアアップデートは提供されていません。

この脆弱性を不正利用するには、攻撃者が内部ネットワークにアクセスしてネットワーク内のデータを傍受する必要があります。このアクセス要件により、エクスプロイトが成功する可能性が制限される可能性があります。

シスコはCVSSスコアを通じて、機能的なエクスプロイトコードが存在することを示していますが、このコードが一般に公開されることは確認されていません。

該当製品

影響を受ける製品バージョンの完全なリストについては、Cisco Bug ID CSCus19789を参照して

ください。

脆弱性のある製品

このアラートが最初に公開された時点では、Cisco Jabber Guest Serverバージョン10.5.0に脆弱性が存在していました。他のバージョンのCisco Jabber Guest Serverも影響を受ける可能性があります。

脆弱性を含んでいないことが確認された製品

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

回避策

今後のアップデートやリリースについては、ベンダーに問い合わせることをお勧めします。

影響を受けるシステムを監視することを推奨します。

管理者は、IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけが該当システムにアクセスできるようにすることを検討できます。

管理者は、信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

修正済みソフトウェア

ソフトウェアの更新プログラムは利用できません。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150106-CVE-2014-8024

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2015年1月6日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。